Making the most of what you have!
Profiling biometric authentication on mobile devices

Sanka Rasnayaka, Sanjay Saha, Terence Sim
School of Computing, National University of Singapore
{sanka, sanjay, tsim}@comp.nus.edu.sg

Abstract

In order to provide the additional security required by modern mobile devices, biometric methods and Continuous Authentication(CA) systems are getting popular. Most existing work on CA are concerned about achieving higher accuracy or fusing multiple modalities. However, in a mobile environment there are more constraints on the resources available. This work is the first to compare between different biometric modalities based on the resources they use. We do this by determining the Resource Profile Curve (RPC) for each modality. This Curve reveals the trade-off between authentication accuracy and resource usage, and is helpful for different usage scenarios in which a CA system needs to operate. In particular, we explain how a CA system can intelligently switch between RPCs to conserve battery power, memory usage, or to maximize authentication accuracy. We argue that RPCs ought to guide the development of practical CA systems.

1. Introduction

With the rapid increase of mobile phone usage in day-to-day activities, including banking and e-commerce the security requirement of these devices has increased drastically. However, a recent survey[23] found that users still prefer convenience over accuracy when using authentication methods. In fact, the survey shows that 25% of users prefer not to use any authentication scheme on their mobile devices.

The main reason for the lack of convenience in traditional authentication schemes is due to the inherent difference in the usage of mobile devices when compared with desktop PCs. The session duration on a desktop PC is much longer compared to that on a mobile device. Therefore the overhead of authenticating for shorter sessions is a higher burden to the user.

It thus seems that security is always at the expense of convenience; but the promise of Continuous Authentication (CA) is to achieve increased security *and* convenience.

Traditional biometric authentication method includes sensing a biometric signal, extracting features from the signal and using a classifier on the extracted features. In a CA system, this process is repeated periodically (say, every 30 seconds) to allow the mobile device to determine the continued presence of the authorized user at any given time. This is illustrated in Fig 1. To do this, the CA system should calculate P, the probability that the user is still present at the device. This provides a higher level of security than traditional session based authentication systems, which would be vulnerable to session hijacking since mobile devices can be easily shared. CA systems rely on passive biometric signal acquisitions, this reduces the disruptions of an active authentication method. For an example, interruptions prompting the user to provide a fingerprint is too disruptive for CA. Other key considerations that should be considered in a CA system is explained in [27].

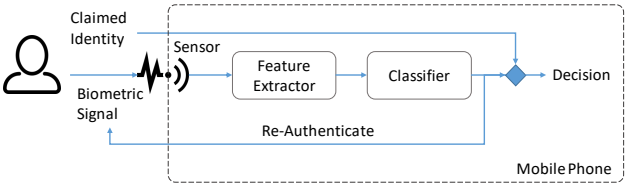

Figure 1. Flow of a Continuous Authentication System

However, compared to desktop PCs, mobile devices are resource-constrained. They have limited amount of energy, computational capabilities, and memory. Continuously checking biometric signals would be an additional strain on these limited resources. Therefore CA researchers should be more aware of how different biometrics consume resources and how to effectively manage these resources.

This work provides an insight into how common transparent biometric modalities consume resources. Our work is focused on understanding the different levels of security each biometric can provide and the resources used to provide that, which can be characterized by a Resource Profile Curve(RPC). This is a first of its kind analysis allowing to compare between biometric modalities based on their re-

978-1-7281-3640-0/19/$31.00 ©2019 IEEE

Modality	Feature Extraction		Classification	
	Feature	Parameters	Classifier	Parameters
Face	PCA[30]	# of PCs	SVM	-
	Fisher[2]	# of components	Random Forest	Depth, estimators
	LBPH[1]	Radius, Neighbours	Neural Network	Number of neurons
	CNN (VGG) [20]	-	Deep CNN (VGG)	-
Voice	MFCC[7]	# of cepstrum filters	GMM	-
	MFCC delta[7]	# of cepstrum filters		
	LOGFBANK[18]	Number of filters	SVM	-
	LPC[19]	Number of order		
Touch	Statistical Features[11]	Number of features	SVM	-
			Random Forest	Depth, estimators
			Neural Network	Number of neurons
Gait	Statistical Features[4]	-	SVM	Soft-margin
			Random Forest	Depth, estimators
			K-Nearest Neighbor	K
			Decision Tree	Max-depth
Soft/Geometric Face Features	Skin color	Skin patch size	Cosine Similarity	-
	5 landmark based geometric features	-	SVM	-
	68 landmark based geometric features	-	Neural Network	Number of neurons
			Random Forest	Depth, estimators

Table 1: Different configurations of biometric algorithms implemented

source usage and the utility (security) they provide.

The proposed Resource Profile Curves will have real-life implications for CA implementations. Following scenarios explain how an RPC for energy consumption will be useful,

- **Security-First** Based on the current application used, a security requirement range can be imposed. (Banking apps requiring higher level of security).
- **Resource-First** Based on the current energy saver mode in the mobile phone, a range of energy consumption which is acceptable can be imposed. (This could mean restricting access to higher security requiring applications)
- **Context Based** Based on context some modalities might not be available requiring the CA system to rely upon the next best alternative. (Face being unavailable due to low light, voice being unavailable due to background noise)

By understanding how each biometric modality performs within resource constraints a CA system can provide the highest possible security while maintaining the lowest possible resource consumption.

2. Literature Review

Since mobile devices are resource constrained, especially in energy and memory, there have been many studies on analyzing and profiling these resources for different aspects (e.g. apps, embedded software etc.). In [22] Qian et. al. did a resource usage profiling for mobile devices in different layers (transport layer, application layer etc.) of a mobile device and proposed a resource optimizer. In [9] Falaki et. al. proposed a smartphone resource usage monitoring tool which measures usage context (CPU and memory) for research deployments. A similar usage measurement tool was proposed by Wagner et. al. in [29] which collects usage based information from Android smart phones and quantifies resource usage by the collaborators.

Carroll et. al. carried out a direct approach to measure the significance of energy drawn by components in a smartphone in [3], where they have analyzed the energy consumption as well as battery lifetime for usage patterns. Tiwari et. al. in their work[28] proposed a power analysis technique which has been applied to two commercial microprocessors for embedded software. In the earlier stages of smart phones, researchers from Nokia came up with a software profiling tool[6] that could be used by developers to measure the power consumption of their applications. The interest in understanding resource usage and minimizing it is evident by the focus on this area of research. However, no light has been shed on profiling of these limited resources for biometrics for mobile devices yet.

CA for mobile devices using biometrics has been getting significant attention [21, 11, 10]. Initial work focused on using a single biometric to implement CA [24, 8, 16, 12],

Dataset	Modalities	Identities	Sessions
MOBIO[17]	Video, Audio	152 total	2 sessions, 6 rounds each
Touchalatics [11]	Smartphone touch	40 people	1
HuGaDB [4]	Accelerometer data	18 people	Variable number

Table 2: Datasets used

later multiple modalities have been fused to achieve higher accuracies[25, 15, 13, 26]. Even though many analysis has been done on usability and security of CA [23, 5, 14], no work has been done on how CA strains a device with limited resources. Our work tries to address this gap and provide a new dimension to answer the question, which modalities we should use based on available resources.

3. Methodology

Throughout this study, the focus is on generating a curve for resource consumption vs utility of biometric modalities. The utility/security provided by the biometric modality can be measured in terms of the algorithm accuracy. This performance will depend on two main factors,

1. Uniqueness of the Biometric. (while hard biometrics like fingerprint/iris could distinguish individuals with higher confidence, behavioural biometrics like GAIT will not have such a level of distinctiveness)
2. Feature extraction and classification algorithms effectiveness.

Based on these factors different biometrics will perform differently on accuracy levels, computational requirements, energy consumption, and memory requirements. We will be measuring these factors to come up with Resource Profile Curves for biometric modalities measured.

3.1. Biometric Algorithms

In order for a biometric modality to be suitable for use in a CA scenario, the signal acquisition should be passive and non-intrusive. Therefore some physiological biometrics like fingerprint and iris are not suitable as they are implemented today because they require users active cooperation to capture. In our study, we have selected *1) Face, 2) Voice, 3) Touch Screen Gestures, 4) GAIT and 5) Soft/Geometric Face Features* as the biometric modalities which allow the acquisition to be done transparently.

In order to characterize the resource consumption vs utility of each of these biometric modalities, some of the popular implementations for these biometric modalities were selected and implemented.

Table 1 summarizes the variations for these biometrics which were analyzed. Multiple combinations of features, classifiers along with variations of the indicated parameters were used to get different configurations of algorithms for each modality. These different configurations will later be profiled in terms of energy consumption and memory consumption to get their Resource Profile Curves.

3.2. Datasets

In order to test all of the different algorithms on a fair grounds we needed a dataset which provides input for all 5 modalities. Since there is no existing dataset that satisfies the requirement, we combined 3 different datasets as shown in Table 2 to create virtual identities.

A key consideration when selecting the datasets was that, they have to emulate the realistic complexity of biometric modalities captured within a mobile environment for CA. Therefore all the datasets were selected to be captured in mobile phones and in usual usage scenarios.

In order to keep the datasets in a similar complexity, we ensured the number of different identities was kept similar. To achieve this we used the IDIAP collection (26 identities) data on MOBIO and entire datasets of Touchalatics and HuGaDB(40 and 18 identities).

3.3. Resource Profile Curves (RPC)

The objective of the work is to come up with a curve for resources consumed vs utility provided by each biometric modality. Here the utility for any biometric is the level of security that modality is able to provide. The level of security will be measured by classification accuracy.

The ideal RPC would be an inverted "L" shape, where the perfect accuracy can be achieved with the minimum amount of resources. The worst case RPC would be a horizontal line on the x-axis where regardless of the resources consumed the accuracy remains at a minimum. However, in reality, the worst case is lower-bounded by the random guessing algorithm.

Each of the algorithm configurations can be plotted with respect to accuracy vs resource consumption in a scatter plot. Let,

$$S = \{\text{(resource, accuracy) pairs for each modality}\} \quad (1)$$

Using the points in S an RPC needs to be generated. In order to generate this the following observations were used,

- The least energy consuming algorithm will be a random guess which will also give the lowest accuracy
- For any limit in available resource level, the algorithm which provides the best accuracy for a lower resource consumption level will be selected

Therefore, the Resource Profile Curve will be lower bounded by the random guessing algorithm. Any new

points in the RPC should be to the right and above this random point. Therefore the RPC will be a monotonically increasing curve.

To generate the RPC the critical points for each modality will be selected using the method shown in the Algorithm 1. Here $p.RC$, $q.RC$ refers to the resource consumption and $p.acc$, $q.acc$ refers to the accuracy of p and q.

Input: S = {Points in the scatter plot}
Output: Sc = {Critical points}
Let Sc = { };
foreach $p \in S$ **do**
  $critical = True$
  foreach $q \in S \mid q.RC \leq p.RC$ **do**
    if $p.acc \leq q.acc$ **then** $critical = False$;
  end
  if $critical = True$ **then** $Sc.add(p)$;
end

Algorithm 1: Isolating critical points

The Resource Profile Curve will be drawn using the pairwise linear curve on the critical points in Sc generated as shown in the algorithm. Following the same method, two Resource Profile Curves were generated,

- Accuracy vs Energy consumption (EC) Profile
- Accuracy vs Memory consumption (MC) Profile

3.3.1 Measuring Energy Consumption (EC)

The overall energy consumption for an authentication task can be analyzed in two parts,

1. EC of the algorithm to perform authentication
2. EC of the sensor to acquire the biometric signal

Energy consumption (EC) for algorithm Time consumed for recognition by each algorithm configuration was used as a proxy for the EC. The main assumption was that the EC by the mobile device will be proportional to the execution time for each algorithm,

$$Energy \propto Time \quad (2) \qquad Energy = k \times Time \quad (3)$$

Here k is the constant of proportionality.

To calculate k, a simple algorithm with a set number of calculations was executed in the PC as well as the Android environment. The runtime for one instance of the algorithm will then be measured and the rate of discharge of the phone battery will also be measured. These two values will be used in the Eqn. (3) to calculate k.

Energy consumption for acquisition An Android application was developed to continuously log the battery level over time at a constant interval. The discharge rate

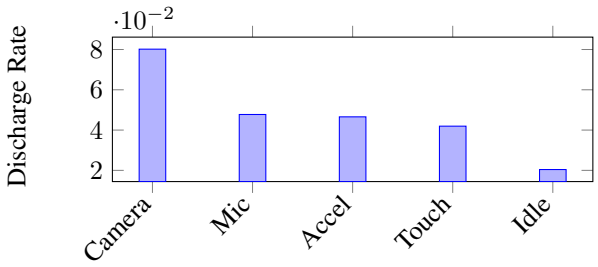

Figure 2. Energy consumption of different sensors

was cealculated for the following: idle, capturing face image every 5 seconds, capturing a voice clip every 5 seconds, logging accelerometer data, logging touch screen data.

In order to isolate the energy discharge rates for biometric signal inputs(RD_{sensor}) the rate of discharge of idle state (RD_{idle}) was deducted from the total rate of discharge ($RD_{measured}$) as shown in Eqn. (4)

$$RD_{sensor} = RD_{measured} - RD_{idle} \quad (4)$$

The energy consumption ($Energy_{algo}$) for a given algorithm can be then calculated as follows,

$$Energy_{algo} = k \times Time_{algo} + R_{sensing} \quad (5)$$

The time consumption was measured on a core i7-6700 3.4 GHz CPU with 8GB of RAM. Mobile battery discharge rates were measured using an LG V10 android device.

The main focus here, is on the time/energy consumed in the test environment. The time consumption for training the models is not considered because in practice training will be done only once, when registering the user of a smartphone. However, the test scenario has to be run on the mobile devices continuously to achieve CA.

3.3.2 Measuring Memory Consumption

The total sizes of feature extraction models (where needed) and classification models were added up for each configuration to measure the memory consumption of each method.

4. Results

The rate of discharge results is shown in Fig. 2. The highest energy consuming sensor is the camera and the lowest energy consuming sensor is the touch screen sensor.

4.1. Calculating Energy Consumption

To calculate the constant of proportionality (k) a simple number addition algorithm was implemented in both computer and mobile platforms and the time and energy discharge rates were measured and the value for k was calculated using the Eqn. (3). The value for k was a very high

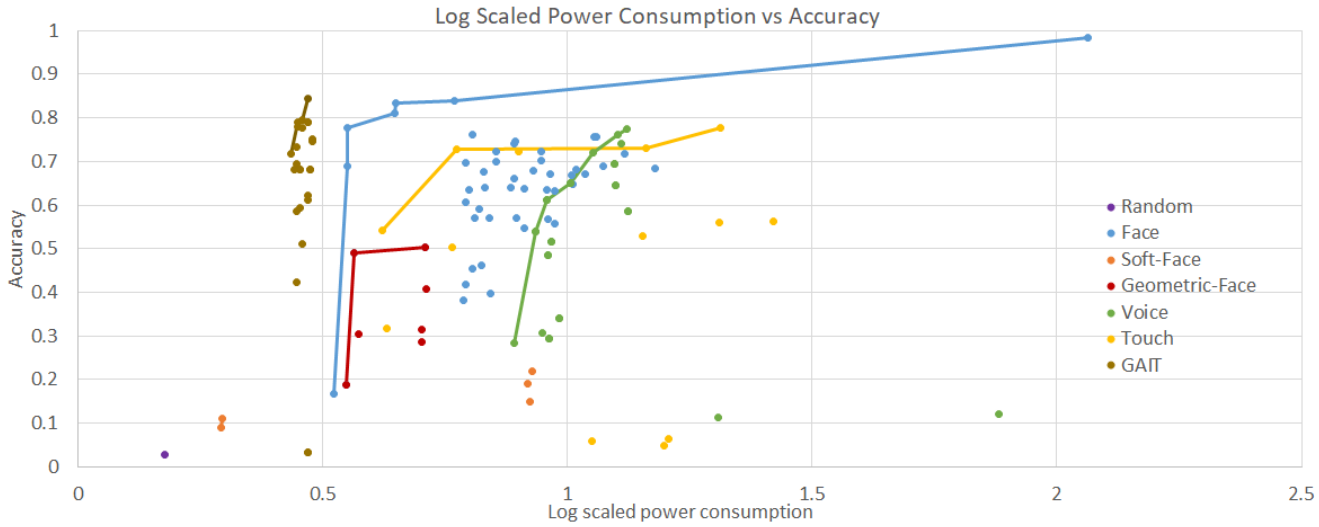

Figure 3. Energy profile for different biometrics

value ($\geq$ 150). Therefore, based on Eqn. (5) the time consumption of the algorithms would dictate the behavior of the curve and hence, the energy consumption of sensing action has a minimal effect.

4.2. Accuracy vs Energy Consumption Profile

Fig. 3 shows the energy consumption vs accuracy curve. The x-axis has been log scaled in order to expand the smaller values and compress the larger values.

All the curves start with a low energy consumption, low accuracy state and they provide higher accuracy with increasing energy consumption. The curves eventually flatten out as energy consumption increases, this shows diminishing returns as the amount of energy consumed is increased.

It can be observed that GAIT outperforms most biometrics in low energy consumption, however, Face biometric outperforms all of the other modalities for highest accuracy achieved. The highest performing algorithm configuration for Face (VGG) consumes roughly 3 times the energy of the 2^{nd} best Face-based user recognition algorithm.

The random point shown in the graph is a baseline for the lowest energy consumption and lowest accuracy, it can be observed that by increasing a very small amount of energy we can achieve a slight increase in accuracy by using soft biometric traits (skin color).

4.3. Accuracy vs Memory Consumption Profile

Fig. 4 shows the memory consumption vs accuracy curve, similar to the previous graph this graph's x-axis has also been log-scaled.

When considering memory constraints there is no clear leader. We can achieve a better than random accuracy without having to save a trained model by using soft feature-based methods. Looking at the curves we can see that voice and GAIT performs best for lower memory values and with larger model sizes face biometrics outperforms the rest.

We will see practical usages of this curve in Section 5.

5. Discussion

5.1. Usage in CA

Comparing Fig. 3 and Fig. 4, complex decisions can be made by a CA system. Depending on the available memory and battery level an intelligent CA system should be able to provide the maximum possible security by using these RPCs. We will illustrate the use-cases highlighted in Section 1 with the generated Resource Profile Curves here,

Security-First

Higher security requiring applications like Banking would require a high-security level (say, accuracy levels over 0.9). Using the RPCs in Fig. 3 4 it is clear that, in order to achieve this level of accuracy the CA system can enforce the use of Face biometric. If unable to capture Face passively the CA system could prompt the user to explicitly provide an authentication before allowing access.

When using an application like YouTube the security requirement is comparatively lower. In a scenario like this, according to the RPC in Fig. 3 the CA system can limit power consumption by using GAIT or Soft-Face biometrics. The CA system can limit the memory consumption by using RPC in Fig. 4 to select Voice or GAIT.

Resource-First

Modern smartphones allow the user to select an energy saver mode, which would activate when the battery level of the device drops below a specified level. In a scenario like this, a CA system can operate in a lower region of the x-axis

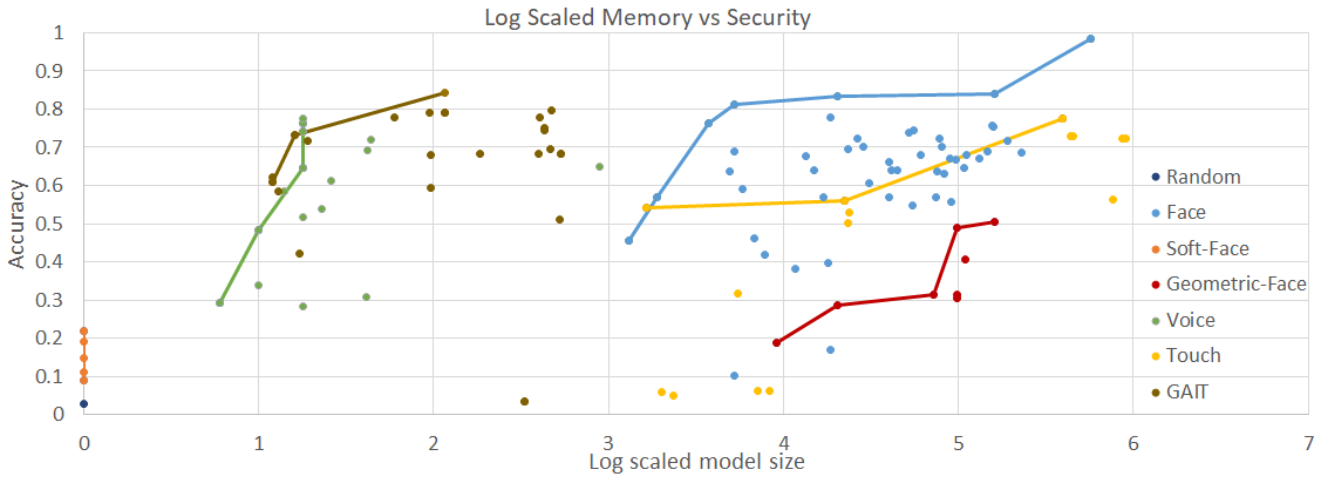

Figure 4. Memory profile for different biometrics

in the energy profile curve in Fig. 3.

A mobile device has a limited amount of free memory. If the available memeory is low, CA system can use the memory profile curve in Fig. 4 to operate in a lower region of the x-axis. By choosing modalities like Soft-Face, GAIT and Voice the CA system can minimize the use of memory.

It is important to note that the RPCs shown here are for unimodal systems. Multiple points in these RPCs could be fused together to achieve higher levels of accuracy at higher resource consumption levels. There is also a trade-off between memory and energy which can be taken advantage of based on the resource limitations.

Context based

Based on the current context the mobile device is being used, the availability of the modalities will change. Following two examples illustrate these scenarios.

1. Walking while answering a call: In this scenario only voice and GAIT modalities will be available.
2. Sitting down, scrolling through an article: In this scenario only Face and Touch modalities will be available

In any of these scenarios, using the RPC, a CA system can find comparable algorithms for the available modalities. The modality selection can be based upon the security required. If the accuracy required is around 0.7, by looking at Fig. 3 we can see that there are comparable algorithms for GAIT, Face, Touch and Voice for this accuracy level.

For an example, when trying to select a biometric modality for CA when face and GAIT are unavailable (due to low light, sensor occlusion in a stationary use-case) the choice will depend on the level of accuracy needed. If the level of accuracy needed is around 0.3, the best alternative would be Soft-Face; if the accuracy requirement is around 0.6, the best alternative would be Touch and if the accuracy requirement is over 0.75 the only option would be Voice. This illustrates how the RPC enables smart choices for a CA system.

5.2. Limitations

The complexity of the datasets can affect the measurement of the Resource Profile Curves. To minimize the impact of this we chose the datasets to be comparable to actual usage in CA for mobile devices. For a given algorithm, the energy consumption will not vary based upon the dataset, however, the accuracy levels will vary based on the dataset. Therefore each modality can be represented by a band of values more completely than the current curves.

As technology improves these curves will keep changing. However, it is clear that the curves can only keep moving up (achieving higher accuracy) and left (consuming lower resources). Therefore we can view these curves as a snapshot view of the biometric modalities. For an example, by looking at the Face RPCs in both Fig. 3 and 4 we can see that there is potential to try and reduce the memory consumed by Face-based authentication algorithms.

6. Conclusions & Future Work

The two RPCs generated in this work provides a new perspective towards evaluating the suitability of biometrics for constrained environments like mobile devices. It is important to note that these curves will keep shifting as the algorithms and hardware improve.

One of the future work is to extend the curves into bands of values by varying the complexity of the datasets as discussed in Section 5.

Another target is to use these Resource Profile Curves in an intelligent decision-making engine to dynamically switch between biometric modalities depending on their availability, resource availability and security requirement.

References

[1] T. Ahonen, A. Hadid, and M. Pietikainen. Face description with local binary patterns: Application to face recognition. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, (12):2037–2041, 2006.

[2] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. Technical report, Yale University New Haven United States, 1997.

[3] A. Carroll, G. Heiser, et al. An analysis of power consumption in a smartphone. In *USENIX annual technical conference*, volume 14, pages 21–21. Boston, MA, 2010.

[4] R. Chereshnev and A. Kert'esz-Farkas. Hugadb: Human gait database for activity recognition from wearable inertial sensor networks. In *International Conference on Analysis of Images, Social Networks and Texts*, pages 131–141. Springer, 2017.

[5] N. Clarke, S. Karatzouni, and S. Furnell. Flexible and transparent user authentication for mobile devices. In *IFIP International Information Security Conference*, pages 1–12. Springer, 2009.

[6] G. B. Creus and M. Kuulusa. Optimizing mobile software with built-in power profiling. In *Mobile Phone Programming*, pages 449–462. Springer, 2007.

[7] S. B. Davis and P. Mermelstein. Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences. *ACOUSTICS, SPEECH AND SIGNAL PROCESSING, IEEE TRANSACTIONS ON*, pages 357–366, 1980.

[8] M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 306–311, Oct 2010.

[9] H. Falaki, R. Mahajan, and D. Estrin. Systemsens: a tool for monitoring usage in smartphone research deployments. In *Proceedings of the sixth international workshop on MobiArch*, pages 25–30. ACM, 2011.

[10] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 451–456. Citeseer, 2012.

[11] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on*, 8(1):136 –148, 1 2013.

[12] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck. Continuous authentication on mobile devices by analysis of typing motion behavior. In *Sicherheit*, 2014.

[13] R. Johnson, R. Murmuria, A. Stavrou, and V. Sritapan. Pairing continuous authentication with proactive platform hardening. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 88–90, March 2017.

[14] H. Khan, U. Hengartner, and D. Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *SOUPS*, pages 225–239, 2015.

[15] R. Kumar, V. V. Phoha, and A. Serwadda. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8, Sept 2016.

[16] H. Lu, A. Brush, B. Priyantha, A. Karlson, and J. Liu. Speakersense: Energy efficient unobtrusive speaker identification on mobile phones. June 2011.

[17] C. McCool, S. Marcel, A. Hadid, M. Pietikainen, P. Matejka, J. Cernocky, N. Poh, J. Kittler, A. Larcher, C. Levy, D. Matrouf, J.-F. Bonastre, P. Tresadern, and T. Cootes. Bi-modal person recognition on a mobile phone: using mobile phone data. In *IEEE ICME Workshop on Hot Topics in Mobile Multimedia*, July 2012.

[18] C. Nadeu, D. Macho, and J. Hernando. Time and frequency filtering of filter-bank energies for robust hmm speech recognition. *Speech Communication*, 34(1-2):93–114, 2001.

[19] D. O'Shaughnessy. Linear predictive coding. *IEEE Potentials*, 7(1):29–32, Feb 1988.

[20] O. M. Parkhi, A. Vedaldi, A. Zisserman, et al. Deep face recognition. In *BMVC*, volume 1, page 6, 2015.

[21] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, 2016.

[22] F. Qian, Z. Wang, A. Gerber, Z. Mao, S. Sen, and O. Spatscheck. Profiling resource usage for mobile applications: A cross-layer approach. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, pages 321–334. ACM, 2011.

[23] S. Rasnayaka and T. Sim. Who wants continuous authentication on mobile devices? In *International Conference on Biometrics Techniques Applications and Systems*, 2018.

[24] P. Samangouei, V. M. Patel, and R. Chellappa. Attribute-based continuous user authentication on mobile devices. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8, Sept 2015.

[25] C. Shen, H. Zhang, Z. Yang, and X. Guan. Modeling multimodal biometric modalities for continuous user authentication. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 001894–001899, Oct 2016.

[26] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong. Senguard: Passive user identification on smartphones using multiple sensors. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on*, pages 141–148. IEEE, 2011.

[27] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar. Continuous verification using multimodal biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):687–700, April 2007.

[28] V. Tiwari, S. Malik, and A. Wolfe. Power analysis of embedded software: a first step towards software power minimization. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2(4):437–445, 1994.

[29] D. T. Wagner, A. Rice, and A. R. Beresford. Device analyzer: Understanding smartphone usage. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 195–208. Springer, 2013.

[30] S. Wold, K. Esbensen, and P. Geladi. Principal component analysis. *Chemometrics and intelligent laboratory systems*, 2(1-3):37–52, 1987.